UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/823,278	03/29/2001	Dennis L. Montgomery	042503 0261929	7295

7590 06/24/2005

PILLSBURY WINTHROP
1600 TYSONS BOULEVARD
MCLEAN, VA 22102

EXAMINER	
CALLAHAN, PAUL E	
ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 06/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/823,278	MONTGOMERY	
	Examiner	Art Unit	
	Paul Callahan	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 April 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-49 and 69-74* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,11-13,15,19-23,26,31,41-45 and 69* is/are rejected.

7)☒ Claim(s) *8-10,14,16-18,24,25,27-30,32-40,46-49 and 70-74* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date ~~~ P.C.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Election/Restrictions

1. Applicant's election without traverse of Group I: claims 1-49 and 69-74 in the reply filed on 4-6-2005 is acknowledged.

2. Claims 1-49 and 69-74 are pending in this application and have been examined.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-3, 6, 7, 13, 15, and 69 are rejected under 35 U.S.C. 102(a) as being clearly anticipated by Johnson, European patent Application: EP 1 032 159 A2.

As for claims 1 and 69, Johnson teaches a method of producing a stream of digital data comprising the step of determining a plurality of portions within the stream of digital data (abstract, col. 3 lines 40-45), such that a portion of the stream of digital data is encrypted with an encryption key that is capable of being decrypted by a decryption

key and the portion including therein another decryption key capable of decrypting a subsequent portion of the stream of digital data (col. 2 lines 15-25, col. 5 line 50 through col. 6 line 20), and the subsequent portion of the stream of digital data is encrypted with another encryption key that is capable of being decrypted by the another decryption key; and transmitting the stream of digital data, including the portion and the subsequent portion (fig. 1 item 36, col. 3 lines 37-52).

As for claim 2, Johnson teaches a method according to claim 1 wherein the portion and a plurality of subsequent portions comprise the plurality of portions, and each of the plurality of subsequent portions is encrypted with a corresponding another encryption key, and within each of the plurality of subsequent portions, except a last subsequent portion, there is included therein a corresponding another decryption key capable of decrypting the corresponding subsequent portion of the stream of digital data (col. 5 lines 50-67, col. 6 lines 1-45).

As for claim 3, Johnson teaches a method according to claim 2 wherein the encryption key and each another encryption key is different and the decryption key and each another decryption key is correspondingly different (col. 6 lines 1-45).

As for claim 6, Johnson teaches a method according to claim 2 wherein the decryption key and each another decryption key are located at a different location within each portion (col. 6 lines 1-45).

As for claim 7, Johnson teaches a method according to claim 2 wherein each portion has a different bit size (col. 5 lines 44-45).

As for claim 13, Johnson teaches a method according to claim 1 wherein the another decryption key is encrypted with the encryption key (col. 5 line 50 through col. 6 line 45).

As for claim 15, Johnson teaches a method according to claim 13 wherein the encryption key and each another encryption key is different and the decryption key and each another decryption key is correspondingly different (col. 6 lines 1-45).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 4, 5, 11, 12, 19, 20-23, 26, 31, and 41-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Johnson and Official Notice taken as detailed below.

As for claim 4, Johnson does not teach a method according to claim 3 wherein each encryption key, each another encryption key, each decryption key and each decryption key have a same key length. However Official Notice may be taken that such a step is old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Johnson. It would have been desirable to do so as this would simplify computations needed in the algorithm.

As for claim 5, Johnson does not teach a method according to claim 3 wherein the encryption key and decryption key and certain ones of the another encryption keys and another decryption keys have a different key length. However Official Notice may be taken that the use of such a feature is old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Johnson. It would have been desirable to do so as this would increase the system security and increase the difficulty in obtaining an unauthorized plaintext.

As for claims 11, 19, 42, and 43, Johnson does not explicitly teach a method according to claim 2 further including a marker that immediately precedes the

decryption key and each another decryption key to allow identification of each another decryption key within the portion and subsequent portions, respectively. However Official Notice may be taken that the use of such a marker is old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Johnson. It would have been desirable to do so as this would allow for more rapid data processing by allowing the key to be identified more quickly.

As for claims 12 and 20, the combination of Johnson and the feature of which official Notice has been taken in claim 11, teaches a method wherein each marker and the corresponding decryption key or another decryption key is encrypted in the same manner as the portion in which it is contained (col. 6 lines 1-45).

As for claim 21, the combination of Johnson and Official Notice teach the limitations of claim 20, Johnson further teaches that each encryption key is different and each decryption key is correspondingly different (col. 6 lines 1-20).

As for claim 22, Johnson teaches a method according to claim 21 wherein the corresponding decryption key in each different portion is not located at a same part of the portion (col. 5 lines 50-67).

As for claim 23, Johnson teaches a method according to claim 22 wherein each portion has a different size (col. 5 lines 39-41).

As for claim 26, Johnson teaches a method according to claim 1 further including, prior to the step of transmitting the stream of digital data, the steps of: transmitting a decryption key that is capable of decrypting the portion of the stream of digital data (col. 7 lines 40-45). Johnson does not teach receiving an acknowledgement indicating that the decryption key has been properly installed on an end-user computer that will receive the transmitted stream of digital data. However, Official Notice may be taken that the use of such a receipt acknowledgement is a step that is old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Johnson. It would have been desirable to do so as this would allow for greater system security in preventing replay attacks.

As for claims 31 and 41, Johnson teaches a method according to claim 26 wherein the portion and a plurality of subsequent portions comprise the plurality of portions, and each of the plurality of subsequent portions is encrypted with a corresponding another encryption key, and within each of the plurality of subsequent portions, except a last subsequent portion, there is including therein a corresponding another decryption key capable of decrypting the corresponding subsequent portion of the stream of digital data (col. 2 lines 15-25, col. 5 line 50 through col. 6 line 20).

As for claim 44, Johnson teaches a method according to claim 43 wherein the corresponding decryption key in each different portion is not located at a same part of the portion (col. 6 lines 1-45).

As for claim 45, Johnson teaches a method according to claim 44 wherein each portion has a different bit size (col. 5 lines 44-45).

Allowable Subject Matter

7. Claims 8-10, 14, 16, 17, 18, 24, 25, 27-30, 32-40, 46-49 and 70-74 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Andrew Caldwell, can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is: (703) 872-9306. Any inquiry of a general nature or relating to the status of this application or

proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

6-20-2005

Paul Callahan